Highlands
School & Sixth Form

Dare to flourish

Online Safety Policy

APPROVED

Date of last review	November 2023
Next review due	November 2025
Governor Committee	School Standards & Performance

Determination Aspiration Respect Equality

Contents

October 2023 - Updates shown in yellow highlight within the document:

- The cyber-bullying section of our policy includes a section about artificial intelligence (AI), which includes a clause related to the potential misuse of generative AI, such as ChatGPT and Google Bard in relation to 'deepfakes'.
- Reflected changes in Keeping Children Safe in Education (KCSIE) 2023:
  - emphasised the role and responsibilities of the governing board in relation to online safety, particularly around maintaining filtering and monitoring systems and staff training
  - added the responsibility that the DSL holds for the school filtering and monitoring systems
- a bullet point stating that governors should make sure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

1. Introduction

1.1. Scope of the Policy

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's digital technology systems, both in and out of the school.

1.1.1. The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

1.1.2. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

1.1.3. The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data.

1.1.4. In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

1.1.5. The online safety policy is to be enacted in conjunction with Keeping Children Safe in Education and the information and support available in Annex D

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

1.2. What is online safety?

The school’s online safety Policy reflects the importance it places on the safe use of information systems and electronic communications.

1.2.1. Online safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

1.2.2. Online safety concerns safeguarding children and young people in the digital world.

1.2.3. Online safety emphasises learning to understand and use new technologies in a positive way.

1.2.4. Online safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.

1.2.5. Online safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

1.2.6. Online safety Policy reflects the importance it places on the safe use of information systems and electronic communications.

1.3. Rationale

1.3.1. The requirement to ensure that children and young people can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

1.3.2. A school online safety policy should help to ensure safe and appropriate use.

1.3.3. Highlands School must demonstrate that it has provided the necessary safeguards to help ensure it has done everything that could reasonably be expected of it to manage and reduce these risks.

1.4. Links to other policies

This policy should be read in conjunction with other school policies that relate in some way to online safety to ensure consistency and to ensure that no aspect of safeguarding children in this area is omitted.

The online safety policy should be considered with the below policies.

1.4.1. Safeguarding
1.4.2. Behaviour
1.4.3. Anti-Bullying
1.4.4. Data Protection
1.4.5. Code of Conduct
1.4.6. RSE & PSHE

2. Monitoring the effectiveness and impact of the policy

2.1. The implementation of this online safety policy will be monitored by the school's ICT strategy manager, the senior leadership team and the governors sub committee (school priorities).

2.2. The governor sub committee will receive once a year a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents).

2.3. The online safety policy will be reviewed every two years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

2.4. Should serious online safety incidents take place, the following external persons / agencies should be informed: LA safeguarding officer, chair of governors, LADO, police.

2.5. The school will monitor the impact of the policy using:

2.5.1. logs of reported incidents
2.5.2. monitoring logs of internet activity (including sites visited) / filtering
2.5.3. surveys of students and parents

2.6. All instances of unacceptable behaviour that fall within the remit of this policy should be reported using the school's agreed systems including Bromcom for behaviour and CPOMS for safeguarding matters.

3. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

3.1. The school online safety coordinators are the:

3.1.1. ICT strategy manager

3.1.2. Designated Safeguarding Lead

3.2. The member of the governing body responsible for online safety is the nominated safeguarding governor

3.3. Governors

3.3.1. Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the governors receiving regular information about online safety incidents and monitoring reports.

3.3.2. Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures

3.3.3. The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

3.3.3.1. Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;

3.3.3.2. Reviewing filtering and monitoring provisions at least annually;

3.3.3.3. Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;

3.3.3.4. Having effective monitoring strategies in place that meet their safeguarding needs.

3.3.4. A member of the governing body will take on the role of online safety governor.

3.3.5. The role of the online safety Governor will include:

3.3.5.1. meeting once a year with the online safety coordinators

3.3.5.2. reporting to Governors School Priorities committee at least once a year

3.4. Headteacher and senior leaders

3.4.1. The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety coordinators.

3.4.2. The headteacher and senior leaders must be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

3.4.3. The headteacher is responsible for ensuring that the online safety co-ordinators and all other members of staff receive suitable training to enable them to carry out their online safety roles.

3.4.4. The headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

3.4.5. The senior leadership team (SLT) will receive once a term monitoring reports from the SLT safeguarding lead at operational meetings.

3.5. The SLT Safeguarding Lead is responsible for:

3.5.1. and has a leading role in establishing and reviewing the school online safety policies and documents.

3.5.2. ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

3.5.3. Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

3.5.4. providing training and advice for staff and emphasised that technology provides additional means for child protection issues to develop

3.5.5. liaising with the local authority.

3.5.6. liaising with school technical staff.

3.5.7. receiving reports of online safety incidents and creates a log of incidents safeguarding to inform future online safety developments.

3.5.8. regularly monitoring of online safety incident logs.

3.5.9. meeting once a year with the online safety governor to discuss current issues, review incident logs and filtering / change control logs.

3.5.10. attending governor's school priority committee meetings.

3.5.11. reporting once a term to the senior leadership team operational meeting.

The SLT safeguarding lead or a designated member of the safeguarding team should be trained in online safety issues and be aware of the potential serious safeguarding / child protection issues to arise from:

3.5.12. sharing of personal data access to illegal / inappropriate materials

3.5.13. inappropriate on-line contact with adults / strangers

3.5.14. potential or actual incidents of grooming

3.5.15. cyber-bullying

3.6. Strategy manager (technical ICT) is responsible for:

3.6.1. taking day to day responsibility for online safety issues

3.6.2. liaising with school technical staff.

3.6.3. receiving reports of online safety incidents and creating a log of incidents related to technical issues to inform future online safety development.

3.6.4. regular monitoring of online safety incident logs.

3.6.5. regular monitoring of filtering / change control logs and for ensuring that:

3.6.5.1. the school’s technical infrastructure is secure and is not open to misuse or malicious attack.

3.6.5.2. the school meets the safety technical requirements and any local authority online safety guidance that may apply.

3.6.5.3. users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

3.6.5.4. the filtering policy is applied.

3.6.5.5. they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

3.6.5.6. the use of the network / internet / virtual learning environment / remote access / e-mail is regularly monitored in order that any misuse or attempted misuse can be reported to the headteacher and online safety coordinators.

3.6.5.7. monitoring software / systems are implemented and updated as agreed with the headteacher.

3.7. Teaching and Support Staff are responsible for ensuring that:

3.7.1. they have an up-to-date awareness of online safety matters and the current school online safety policy and practices.

3.7.2. they have read, understood, and signed the staff acceptable use agreement (AUA).

3.7.3. that they report any suspected serious misuse to safeguarding lead for investigation / action / sanction all digital communications with students / parents / carers should be on a professional level and only carried out using school systems.

3.7.4. online safety policy is adhered to in all aspects of the curriculum and other activities.

3.7.5. students understand and follow the online safety and acceptable use agreements.

3.7.6. students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

3.7.7. they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices.

3.7.8. in lessons where internet use is pre-planned, students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.7.9. in all lessons where computers are available for pupil whole class use, including cover lessons, staff will use monitoring software.

3.8. Students:

3.8.1. are responsible for using the school digital technology systems in accordance with the student acceptable use agreement.

3.8.2. have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

3.8.3. need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

3.8.4. will be expected to know and understand policies on the use of mobile devices and digital cameras.

3.8.5. will be expected to know and understand policies on the taking / use of images and on cyber-bullying.

3.8.6. should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school’s online safety policy covers their actions out of school, if related to their membership of the school.

3.9. Parents/Carers

3.9.1. Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through parents’ evenings, letters, website, VLE and information about national / local online safety campaigns and literature.

3.9.2. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

3.9.2.1. digital and video images taken at school
3.9.2.2. access to parents’ sections of the website and online student records
3.9.2.3. their children’s personal devices in the school

4. Training

4.1. Headteacher

4.1.1. The headteacher is responsible for ensuring that the online safety coordinators in school (safeguarding and technical) receive sufficient training to fulfil their role.

4.2. All Staff

4.2.1. In accordance with the wider safe-guarding policy in school all staff have a responsibility for ensuring the highest standards of online safety to allow this to happen.

4.2.2. It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

4.2.2.1. a planned programme of formal online safety training made available to staff.

4.2.2.2. an audit of the online safety training needs of all staff carried out regularly.

4.2.2.3. new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.

4.2.2.4. this online safety policy and its updates will be presented to and discussed by staff on inset days and in meetings when required.

4.2.2.5. the online safety coordinators will provide advice / guidance / training to individuals as required.

4.3. Governors

4.3.1. The safeguarding link governor with responsibility for online safety will be provided with the relevant training as required and will be expected to have access to online safety training as part of the training cycle provided to staff.

4.4. Parents

4.4.1. The school will provide parents with appropriate online safety information and/or workshops on an annual basis.

5. Mobile Technologies

5.1. The school does not accept responsibility for personal devices brought into school or any liability for loss, damage or malfunction following access to the network or wifi. The right to take, examine and search users' devices in the case of misuse is outlined in the Behaviour Policy.

5.2. School devices that are loaned to students are controlled by policies, firewalls and virus scanners and their use is monitored automatically in the same way as school based devices.

5.3. The table below summarises the use and access of portable devices in school:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Access to network servers	Yes	Yes	No	No	No	No
Wifi Internet Access	Yes	Yes	Yes	Yes*	Yes	Yes

* sixth form students computer/tablets only

[1] Authorised device – purchased by the student/family through a school-organised scheme.

6. Education

6.1. Online safety within the curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

6.1.1. a planned online safety curriculum as part of computing, PSHE and citizenship lessons.

6.1.2. key online safety messages reinforced as part of a planned programme of assemblies

6.1.3. in all lessons students taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

6.1.4. in all lessons students taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

6.1.5. in all lessons students supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making

6.1.6. in all lessons students taught to use age-appropriate tools to search for information online.

6.1.7. sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

6.2. Social Networking

6.2.1. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

6.2.2. Students are taught through the computing and PSHE curriculum about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school i.e. being aware of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and behaviour online.

6.2.3. Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run with the approval of a member of staff and will be moderated by a member of staff.

6.2.4. Through regular safeguarding updates and CPD, all staff will be made aware of the professional risks associated with the use of personal social media and guided to ensure privacy options are active.

6.3. Cyberbullying

6.3.1. Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the anti-bullying policy.

6.3.2. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person.

6.3.3. It is made noticeably clear to students and members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

6.3.4. Students are also educated on the dangers of internet grooming/sexting and child abuse. Using real life and scenario situations students are guided with making responsible decisions while using digital equipment.

6.3.5. Students will be educated through the computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

6.4. Artificial intelligence (AI)

6.4.1. Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

6.4.2. The school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

6.4.3. The school will treat any use of AI to bully pupils in line with our behaviour policy.

6.4.4. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Use of digital and video images

7.1. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

7.2. Before photographs of students are published on the school website, social media or local press, staff must check against the list of students whose parents/carers have not given consent for the use of their image. This is held by the reprographics department.

7.3. Photographs of students and student activity should only be made using school owned devices such as mobiles, tablets and laptop computers. Personal devices should not be used.

8. Protecting Professional Indemnity

8.1. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

8.1.1. ensuring that personal information is not published.

8.1.2. training including acceptable use, social media risks, checking of settings, data protection, reporting issues.

8.1.3. clear reporting guidance, including responsibilities, procedures and sanctions

8.1.4. risk assessment, including legal risk.

8.2. School staff should ensure that:

8.2.1. no reference should be made in social media to students, parents / carers or school staff

8.2.2. they do not engage in online discussion on personal matters relating to members of the school community.

8.2.3. personal opinions are not attributed to the school or local authority

8.2.4. security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

8.3. Staff Personal Use

8.3.1. Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

8.3.2. Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

8.3.3. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

9. Acceptable use agreements

All members of our community will be expected to read and sign the appropriate acceptable use agreement on joining the school and at times when the policy is updated.

See Appendix B

10. Responding to inappropriate use

10.1. Inappropriate use within a school context would be deemed to be anything which contravenes the staff or student acceptable user agreement. Breaches of the policy other than illegal incidents will be dealt with in line with the behaviour policy.

10.2. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

10.3. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. These include:

10.3.1. Mobile phone use (visible, using a phone or a phone rings/pings)
10.3.2. Use of other non-permitted electronic devices
10.3.3. Inappropriate use of IT equipment during a lesson eg- playing games, watching videos or looking at websites not related to the lesson
10.3.4. Mobile phone, earphones or other electronic devices use around the school site
10.3.5. Unkind and cruel comments towards another student
10.3.6. Refusal to hand over mobile phone, earphones or other electronic device
10.3.7. Bringing the school into disrepute due to behaviours before or after school
10.3.8. Downloading or bringing into school pornographic material
10.3.9. Requesting/sending/sharing indecent electronic images of/from another person (or printed)
10.3.10. Having indecent images of children/other students on phone or other device
10.3.11. Actions that put the health and safety of any other member of the school community at serious risk

10.4. In the event of suspicion, all steps in this procedure should be followed:

10.4.1. have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

10.4.2. conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. use the same computer for the duration of the procedure.

10.4.3. ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

10.4.4. record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. these may be printed, signed and attached to the serious incident form (except in the case of images of child sexual abuse – see below).

10.5. Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not.

10.5.1. if it does, then appropriate action will be required and could include the following:

10.5.1.1. internal response or discipline procedures.

10.5.1.2. involvement by local authority / academy group or national / local organisation (as relevant).

10.5.1.3. police involvement and/or action.

10.6. Following the investigation, if action is needed then it could include one of the following:

10.6.1.1. sanctions using the behaviour policy, including exclusion.

10.6.1.2. involvement of local authority or national and local organisations (as relevant)

10.6.1.3. police involvement or action.

11. Illegal incidents

11.1. If there is any suspicion that the activities or web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the flowchart below and report immediately to the police.

11.2. If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the police. Other instances to report to the police would include:

11.2.1.1. incidents of ‘grooming’ behaviour

11.2.1.2. the sending of obscene materials to a child

11.2.1.3. adult material which potentially breaches the Obscene Publications Act

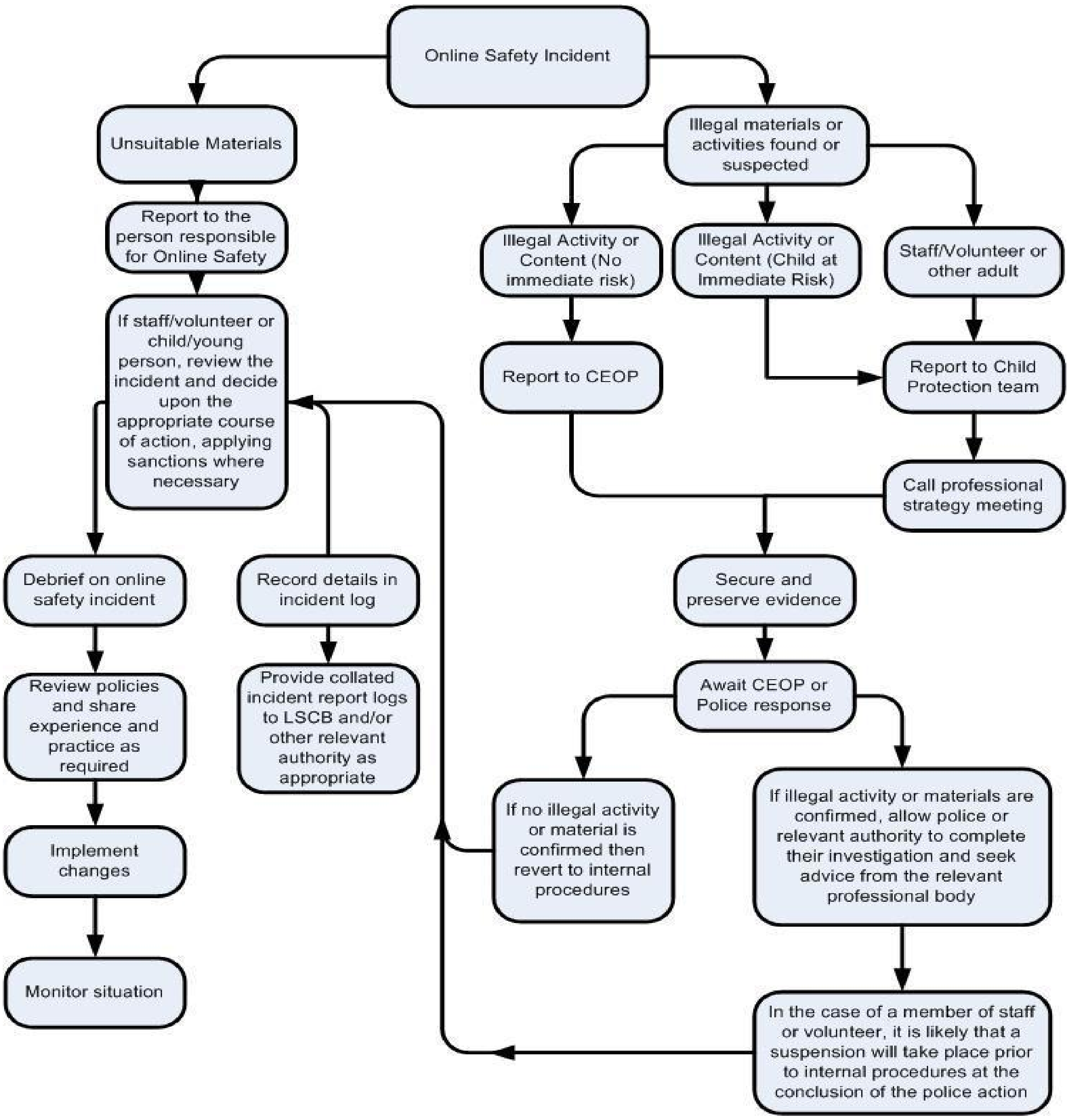
11.2.1.4. criminally racist material

11.2.1.5. promotion of terrorism or extremism

11.2.1.6. other criminal conduct, activity or materials

11.3. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

11.4. It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

12. Communicating this policy

12.1. This policy will be published on the school website, the staff shared network area and made available in printed form from the school office upon request.

12.2. Staff and students will be required to sign the AUA on entry to the school and after revision of the agreement.

12.3. Notice of any changes will be sent by email to parents, staff and students via email.

12.4. A summary of the policy will be displayed on posters around the school.

12.5. The policy will be highlighted for students through an annual online safety week in assemblies and tutor periods.

12.6. The acceptable use agreements will be used to highlight key responsibilities.

Appendix 1 - Acceptable Use Agreements

Highlands School

Information and Communication Technology

Acceptable Use Agreement

This form relates to the Student Acceptable Use Agreement.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

Student Agreement

I have read and understand the above and agree to follow these guidelines:

- When I use the school systems and devices (both in and out of school)
- When I use my own devices in the school (when allowed) e.g. mobile phones, USB devices, cameras etc.
- When I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school online.
- I understand that these rules are designed to keep me safe and that if they are not followed school sanctions will be applied, and my parent carer may be contacted.

Name of Student: ____Form:______

Signed: ____Date:______

Parent/Carer Agreement

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

- I know that my child has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed:____ Date:______

Student Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could compromise the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

A For my own personal safety:

1. I understand that the school will monitor my use of technology and digital communications systems provided by the school. I will not attempt to bypass the internet filtering systems.
2. I will log on to the school network with my own username and password and not allow others to know or use my network account.
3. I will be aware of “stranger danger”, when I am communicating on-line. If I arrange to meet people offline that I have communicated with on-line, I will do so in a public place and take an adult with me
4. I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
5. I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

B I understand that everyone has equal rights to use technology as a resource and:

1. I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
2. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
3. I will not use the school systems or devices for social media, on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

C I will act as I expect others to act toward me:

1. I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
2. I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
3. I will not take or distribute images, videos or sound files of anyone without their permission or in a manner which is designed to upset, harass or intimidate.
4. I will ensure that my online actions do not harm the reputation of the school or school community.

D I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

1. I will not alter the hardware (such as keyboards, mice or other peripheral items) and will report any observed damage, however this may have happened, to a member of staff as soon as possible.
2. I will not download or install software onto school equipment. I will not try to alter computer settings.
3. I will only use my phone in line with the school Mobile Phone Policy.
4. I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

E When using the internet for research or recreation, I recognise that:

1. I should ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not try to download copies (including music and videos)
2. When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

F I understand that I am responsible for my actions, both in and out of school:

1. I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement. This includes incidents when I am out of school and where they involve my membership of the school community (examples would be cyberbullying, use of images or personal information).
2. I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusion, contact with parents and, in the event of illegal activities, involvement of the police.

Staff, Governor and Volunteer Acceptable Use Agreement

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

A Professional and personal safety:

1. I will use the school's ICT facilities, software, hardware and any related technologies for professional purposes only and as deemed acceptable by the Head Teacher.
2. I understand that my use of ICT equipment to access the Internet and other related technologies whilst on school equipment inside or outside of the site will be monitored and logged. This can be made available, on request, to my Line Manager or Head teacher.
3. I will comply with the ICT security practices and not disclose any passwords provided to me by the school or other related authorities. I will not use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
4. I will not engage in any on-line activity that may compromise my professional responsibilities. I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.
5. I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
6. I will not use a personal telephone for personal calls or texting in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room or offices.
7. I will respect copyright and intellectual property rights.

B Professional communications and actions when using school ICT systems:

8. I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner and will ensure sensitive data is sent using agreed encryption (Egress or similar).
9. I will not give out my personal details, such as mobile phone number, email address, social media accounts, to pupils and I understand that exceptions can only be given on a case by case basis by the Head Teacher.

10. I will ensure that personal data (such as data held in SIMS) is kept secure and is used appropriately, whether in school, taken off site or accessed remotely. I understand that personal data can only be taken off site or accessed remotely when authorised by the Head and that such data must be encrypted, e.g. on a password secured laptop or encrypted memory stick.
11. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
12. I will only take, store and use images of pupils or staff for professional purposes in line with school policy and with written consent of the parent, carer or staff member. I will not use my personal equipment to record these images, unless I have permission to do so.
13. I will not distribute images outside the school network without the permission of the parent/carer, member of staff or Head teacher.

C Safe and secure access to technologies and the smooth running of the school:

14. I will support and promote the school's online safety and data policies and help pupils to be safe and responsible in their use of ICT and related technologies.
15. I will always use software provided (e.g. Impero) to monitor ICT use by pupils.
16. I will not install or purchase any hardware or software for use in the school without the permission of the ICT Strategy Manager and I understand that any such permitted hardware or software may not be supported. I will not try to alter computer settings, unless this is allowed in school policies.
17. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
18. I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will immediately report any damage or faults involving equipment or software, however this may have happened.

D Responsibility for my actions in and out of the school:

19. I understand that this Acceptable Use Agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and to my use of personal equipment on the premises or in situations related to my employment by the school
20. I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school information communication technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ____ Role: Staff / Governor / Volunteer

Signed: ________________________________ Date:__________________________

Appendix 2 - Remote Learning

A. During a period of remote learning due to school closures (for example COVID or adverse weather conditions) staff are required to use Google Classroom to communicate with students and to set work.

B. Guidelines for the completion of online activities, including any revised timetable or assessment schedule will be published by the senior leaders for staff to implement.

C. Students will be expected to log on, access and complete work through Google Classroom every school day.

D. Teachers will monitor and report on student activity as required as this will help students to keep up with learning and to maintain a routine that supports their well-being.

E. Meetings originating from school staff with students, parents, carers and other professionals will be conducted using Google Meet.

F. Parent Evenings held remotely will use School Cloud or a similar web based system

Guideline for periods of remote learning

1. Test your audio and video before a scheduled call.
2. Record any live classes so that the video can be reviewed if any issues arise.
3. Be punctual and courteous. Introduce yourself and take note of other attendees' names so you can address them by name. Turn off the call tone on your phone. Treat this just like you would a face to face meeting with a student, colleague or other adult.
4. Conduct yourself in a professional manner throughout the call - you remain an employee of the school throughout the call.
5. Conduct video calls to learners or colleagues from a desk or other appropriate location.
6. Remind students that all audio/video may be recorded, to safeguard both parties and this wouldn't routinely be shared.
7. Make sure to have the current client version loaded before scheduled calls.
8. Look at your screen, pay attention to others and when speaking make sure to look at your camera.
9. Use the 'blur background option' to hide any background if needed.
10. Picture in Picture is your best reference, you can see yourself and your surroundings just as others on the call can.
11. Make sure you have good light. Adjust lighting or use a portable light source to make sure you have good lighting on you from the front without having to look directly into a harsh light, eg: by pointing a strong desk lamp at the wall you're facing.
12. Ensure you are appropriately dressed; 'business casual' at all times.
13. Mute your microphone when not needing to talk to avoid background noise.
14. Keep sessions to a reasonable length and to timetabled activities.

Useful further guidance

TES: Coronavirus: 10 safeguarding rules for teachers at home

NSPCC: Undertaking remote teaching safely

NSPCC: Internet connected devices